(12) UK Patent Application (19) GB (11) 2 155 676 A

(43) Application published 25 Sep 1985

(21) Application No 8504507

(22) Date of filing 21 Feb 1985

(30) Priority data
(31) 84/030315 (32) 22 Feb 1984 (33) JP

(51) INT CL⁴
H04B 5/04 H04L 9/00

(52) Domestic classification
G4H 13D 14A 14D 14G 60 RBE RCE
U1S 2196 2209 G4H

(56) Documents cited
None

(58) Field of search
G4H

(71) Applicant
NEC Corporation (Japan),
33–1 Shiba 5-chome, Minato-ku, Tokyo, Japan

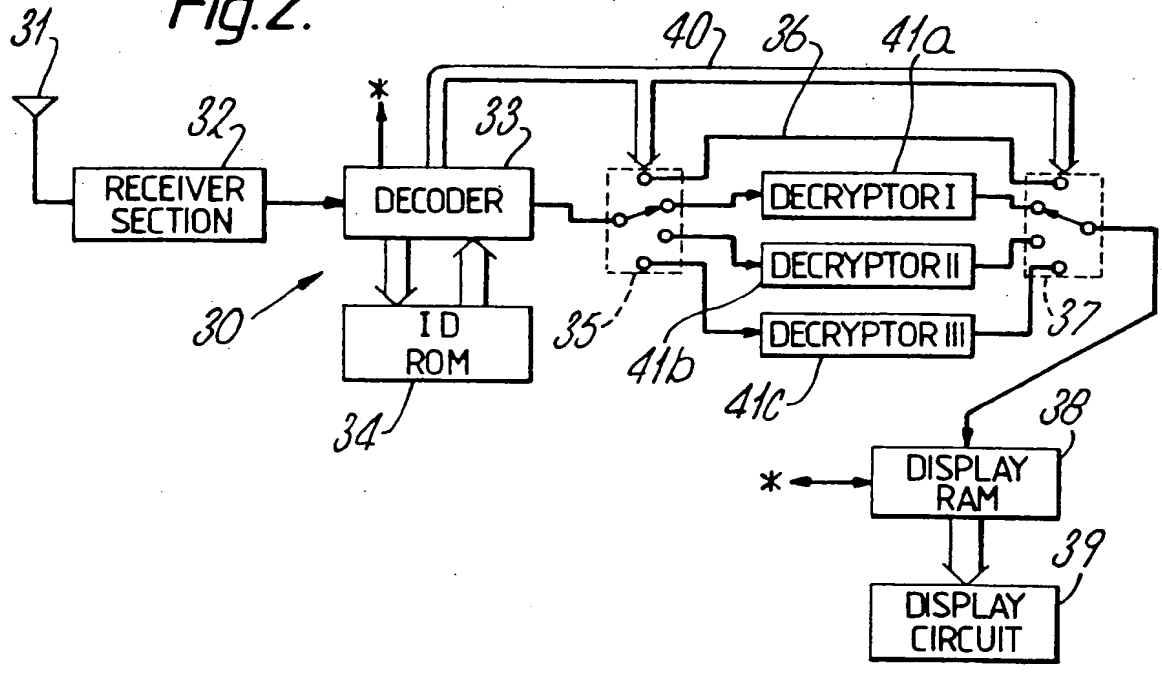
(72) Inventor
Takakuni Kuki

(74) Agent and/or Address for Service
John Orchard & Co,
Staple Inn Buildings North, High Holborn, London
WC1V 7PZ

(54) Paging receiver

(57) A paging receiver comprises: memory means for storing a receiver's own paging number and decrypting information for selecting, out of decrypting methods corresponding to a plurality of encrypting methods, one corresponding to the paging number; receiver means for receiving a paging number and a message following it; decrypting means for comparing the received paging number and the stored paging number and, if they are found identical, decrypting the received message by the decrypting method selected on the basis of the decrypting information; and display means for displaying the decrypted message.

Fig.2.



The drawing(s) originally filed was/were informal and the print here reproduced is taken from a later filed formal copy.

GB 2 155 676 A

INSDOCID: <GB_____2155676A__I_>

Fig.1.

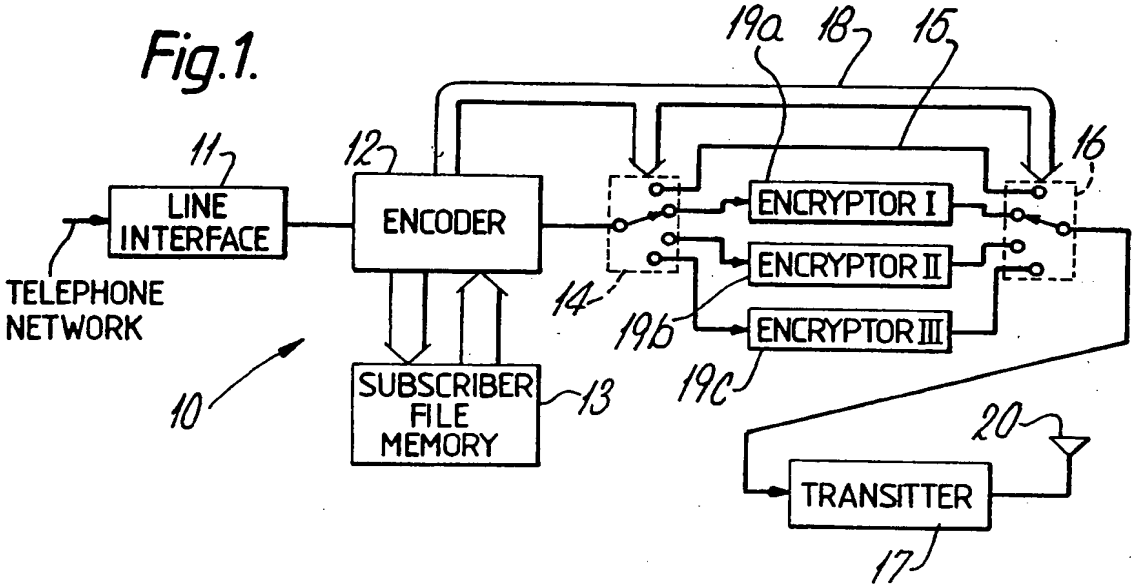
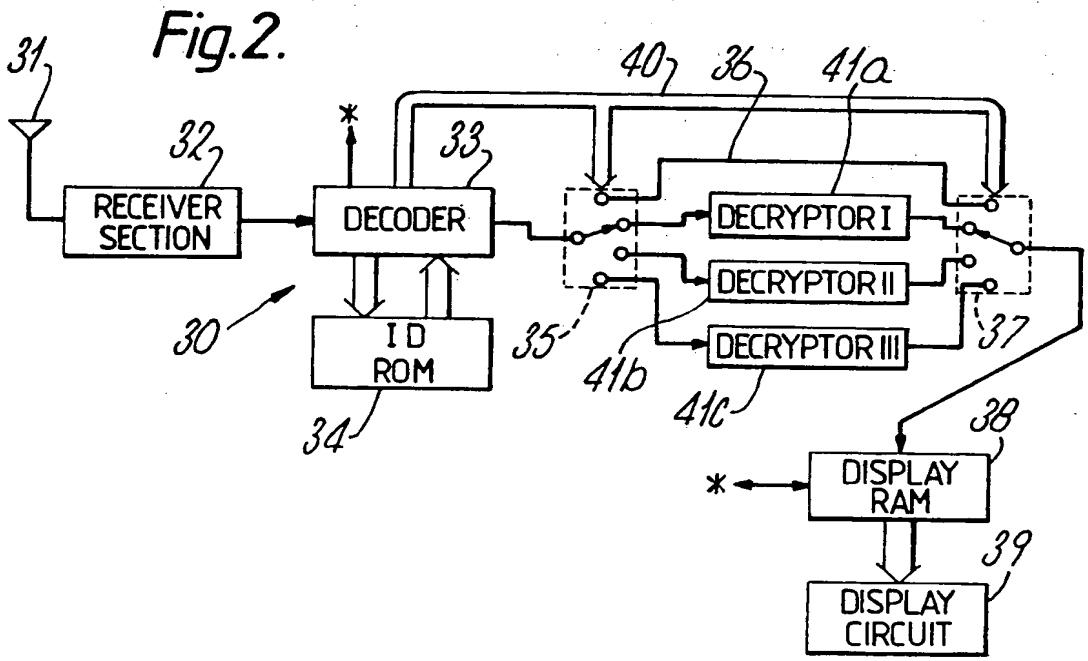


Fig.2.



NSDOCID: <GB 2155676A I >

Fig.3.

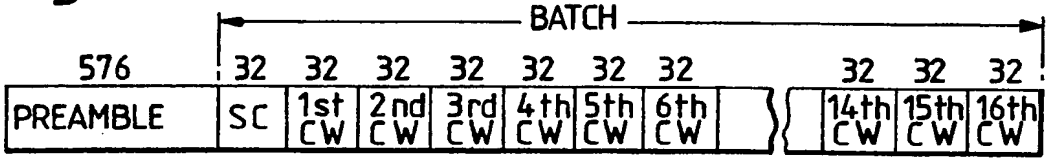


Fig.4A.

Fig.4B.

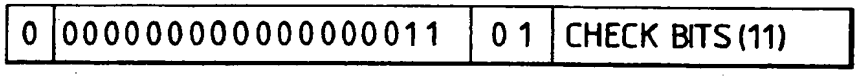


Fig.4C.

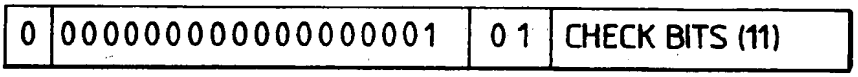


Fig.4D.

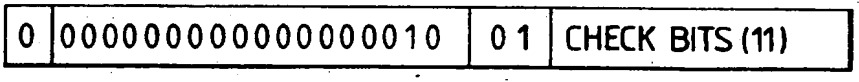


Fig.5A.

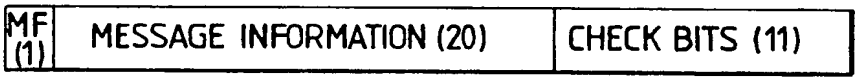


Fig.5B.

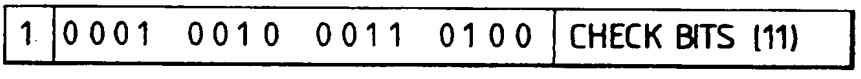


Fig.5C.

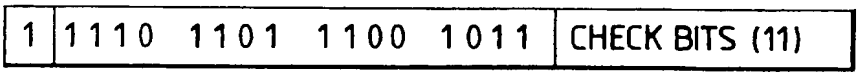
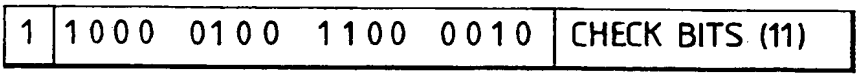


Fig.5D.



3NSDOCID: <GB 2155676A I >

SPECIFICATION

Paging system capable of having a plurality of encryptors and receiver therefor

Background of the Invention

The present invention relates to a radio paging system and, more particularly, to a radio paging system for transmittining information to display-equipped paging receivers capable of being called by unspecified persons.

A radio paging system capable of transmitting messages can transmit the telephone number and name of the caller as a message. Receiving such a message, a display-equipped receiver can identify the caller. Therefore, this kind of receiver can be called by many unspecified persons. As a result, the holder of the receiver usually makes his receiver number known to many acquaintances.

Some calling systems capable of transmitting messages are intended for the very purpose of transmitting messages but not for calling. For instance, if a subscriber to a calling system may want to know current stock quatations, i.e., daily highs, lows, bid prices or trading volume even when out of his office or home, the pertinent prices may be transmitted to him at hourly intervals. If in such an instance personal information or highly confidential information is to be also transmitted as part of the message, there will arise the problem of keeping the message confidential. Thus, since the paging or calling number of the receiver is made known to many persons as stated above, anyone who happens to known the number can readily copy the receiver to eavesdrop the message.

Summary of the Invention

An object of the present invention, therefore, is to provide a radio paging receiver which makes it difficult to eavesdrop or tap the message even if the paging number of the paging receiver is made known to unspecified many.

Another object of the invention is to provide a radio paging receiver which has a plurality of message decrypting or deciphering methods and selects one of them corresponding to the receiver's own paging number.

In an embodiment to be described a paging receiver comprises memory means for storing the receiver's own paging number and decrypting information for selecting, out of decrypting methods corresponding to a plurality of encrypting methods, one corresponding to the paging number; receiver means for receiving a paging number and a message following it; decrypting means for comparing the received paging number and the stored paging number and, if they are found identical, decrypting the received message by the decrypting method selected on the basis of the decrypting information; and display means for displaying the decrypted message.

Detailed Desciption of the Drawings

These and other objects, features and advantages of the present invention will become more apparent from the detailed description hereunder taken in conjunction with the accompanying drawings, wherein:

Figure 1 is a schematic block diagram illustrating one preferred embodiment of the transmitting side of a paging system;

Figure 2 is a schematic block diagram illustrating one preferred embodiment of the receiver of a paging system according to the invention;

Figure 3 shows the structure of a POCSAG code applicable to a system according to the invention;

Figures 4A to 4D show the structure of an address codeword of the POCSAG code; and

Figures 5A to 5D show the structures of a message codeword of the POCSAG code and another resulting from the ciphering of the POCSAG code in accordance with the invention.

Detailed Description of the Preferred Embodiment

In Fig. 1, reference numeral 10 represents a part of an electronic switchboard connected to a public telephone network, which constitutes the transmitting side of a paging system according to the present invention. A line interface 11 connected to the public telephone network receives, and supplies to an encoder 12, the paging number of the paging receiver to be called and message information addressed thereto. The encoder 12 supplies the received paging number to a subscriber file memory 13, and receives therefrom an address codeword and data of either a ciphering or encrypting method (cipher or encryptor), both the address codeword and the data corresponding to the paging number. The subscriber file memory 13 stores an index list of the paging numbers of paging receivers and information on the selection of the encrypting method (encryptor).

When a person intending to carry with him a paging receiver so reports to an agency in charge of radio paging service and is assigned a paging number, he or she designates one out of a plurality of encrypting methods (encryptors). The radio paging service agency writes an index list of the paging numbers of receivers and address codewords into the subscriber file memory 13, together with information to enable the decoder 12 to select one of encrypting methods (encryptors).

The encoder 12 sends the address codeword from the subscriber file memory 13 to a transmitter 17 by way of a switch 14, a connecting line 15 and another switch 16. In accordance with data for encrypting method, the encoder 12 controls the switches 14 and

ISDOCID: <GB 2155676A I >

16 through a data bus 18. The encoder 12 also encodes message information received from the line interface 11 into a message codeword and supplies the message codeword to the transmitter 17 via one of encryptors 19a tp 19c and of the connecting line 15, selected on the basis of encryptor designating information received from the subscriber file memory 13. The transmitter 17, after effecting necessary processing such as frequency shift keying (FSK) modulation and amplification, transmits the address and message codewords by way of an antenna 20 as a paging signal.

In Fig. 2, reference numeral 30 represents a radio paging receiver, which constitutes the receiving side of a paging system according to the present invention. The paging signal from the transmitting side 10, illustrated in Fig. 1, is received by a receiver section 32 through an antenna 11. The receiver section 32 constitutes a demodulator circuit for frequency-modulated (FM) signals, and usually includes the constitutent element up to the frequency discriminator. A received signal is demodulated by the receiver section 32 into a base-band signal and led to a decoder 33. The encoder 33 shapes the waveform of the base-band signal to provide a binary signal. Thus, the encoder 33 provides demodulated address and message codewords. Then, the encoder 33 compares the demodulated address codeword and the receiver's own address codeword stored in an ID read-only memory (ROM) 34, drives an alert tone generator (not shown) to generate an alert tone if the two address codewords are found identical, and takes in the ensuing message codewords.

ID ROM 34 stores the receiver's own address codeword and information commanding decryption of an encrypting method (decryptor) corresponding to the address codeword, i.e., the receiver's own paging number. The decoder 33 changes over, by way of a data bus 40, switches 35 and 37 on the basis of decrypting method-designating information supplied from the ID ROM 34, and transfers the message codeword to one of a connecting line 36 and decryptors 41a to 41c. The message codeword is supplied to a display randon access memory (RAM) 38 either directly via the connecting line 36 or after being decoded by the decryptor 41a, 41b or 41c. The message from the RAM 38 is displayed on a display circuit 39. The RAM 38, under the control of the decoder 33, also operates when recalling the stored messages as controlled with a manual switch (not shown) connected to the decoder 33.

Fig. 3 is a compositional diagram of a paging or calling code known as the POCSAG code, proposed by British Telecom in June 1978 and November 1980 and described in "Report of the Post Office Code Standardization Advisory Group (POCSAG)." The paging code begins with a preamble signal consisting of 576 bits, followed by a batch including a 32-bit synchronization codeword (SC) and 16 32-bit addreess or message codewords (CW). There may be more than one batch, depending on the relative congestion of calls. For details on the POCSAG code, reference may be made to the above cited report.

Figs. 4A to 4D are an enlarged diagram and examples of the address codeword, and Figs. 5A to 5D, those of the message codeword. In these figures, a one-bit message flag MF indicates whether the codeword concerned is an address or message codeword; if it is "0" the codeword will be an address codeword, or if it is "1", the codeword will be a message codeword. In Figs. 4A to 4D, 18 bits immediately following the message flag MF are address bits, representing the paging number of the receiver in binary digits. The next two are function bits FB, "00" indicating that the address codeword is followed by no message; "01" abd "10" which are used to select the required address from the two assigned to the receiver, indicating that the address codeword is followed by a numerical (numeric-only) message; and "11" indicating that the address codeword is followed by an alpha-numeric or general message. The final 11 bits are check bits, used for detection and correction of errors owing to noise or the like.

In Figs. 5A to 5D, while the final 11 bits are the same check bits as in the address codeword, 20 bits following function bits FB constitute message information, the information to be displayed. In this instance, the message information in Figs. 5B to 5D is shown as what respectively follows Figs. 4A to 4B. The message information in every case is of four numerals "1, 2, 3, 4". Figs. 4B and 5B illustrate a case wherein the paging number is "3" and the message is transmitted without encryption (i.e. via the connecting line). Figs. 4C and 5C show another wherein the paging number is "1" and the message is transmitted to the receiver after being encrypted to "invert logic 1 and 0". For example, a binary code "0001" is inverted to "1110." Figs. 4D and 5D represent still another wherein message is transmitted to a receiver bearing the paging number of "2" after being encrypted to "reverse the order in every four bits". For example, a code "0001" is reversed to "1000" or a code "0010" to "0100". Therefore, if for instance the subscriber of No. "2" alters his paging number to "1", he will not be able to receive a correctly decrypted message because of the difference in the encrypting method of message information.

Although only 20 message bits out of the whole message codeword are encrypted in the foregoing example, it also is possible to encrypt the whole message codeword without

INSDOCID: <GB_____2155676A__I_>

the message flag (MF) bit. It has further to be noted that the methods of encryption are not limited to "inversion" and "reversing the order", but many others are also conceivable. The encryptors and decryptors are constructed by hardware; however, they may be composed of software.

The radio paging system according to the present invention enables any properly registered bearer of a receiver to receive calls and messages as readily as one of a receiver not using this system, but it would be practically impossible for any other person to eavesdrop the message transmitted. The potential eavesdropper could readily find out the paging number of the legitimate bearer of the receiver, but it would be virtually impossible for him or her to decrypt the message even if he has a receiver of the same type because the paging number would give him no hint as to the method by which the message is encrypted.

CLAIMS

1. A paging reciever comprising:

memory means for storing the receiver's own paging number and decrypting information for selecting, out of decrypting methods corresponding to a plurality of encrypting methods, one corresponding to said paging number;

receiver means for receiving a paging number and a message following it;

decrypting means for comparing the received paging number and the stored paging number and, if they are found identical, decrypting the received message by the decrypting method selected on the basis of said decrypting information; and

display means for displaying the decrypted message.

2. A paging receiver, as claimed in Claim 1, wherein said decrypting means comprises a plurality of decryptors respectively corresponding to said decrypting methods; switching means for switching these decryptor; and decoder means for performing the comparison of said paging numbers, driving said switching means and selecting one of said decryptors on the basis of said decrypting information, and supplying said received message to the selected decryptor.

3. A paging receiver, as claimed in Claim 1, wherein said encrypting methods include the bit inversion method.

4. A paging receiver, as claimed in Claim 1, wherein said encrypting methods include the bit order reversal method.

5. A paging receiver, as claimed in Claim 1, further including display memory means, connecting between said decrypting means and said display means, for temporarily storing said decrypted message.

6. A paging receiver, as claimed in Claim 5, wherein said display memory means includes a random access memory.

7. A paging receiver substantially as described herein with reference to Fig. 2 of the accompanying drawings.

Printed in the United Kingdom for
Her Majesty's Stationery Office, Dd 8818935, 1985, 4235.
Published at The Patent Office, 25 Southampton Buildings,
London, WC2A 1AY, from which copies may be obtained.

VSDOCID: <GB_____2155676A_I_>